Ilari Kontio

Yritysverkon toteutus

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

15.4.2014

Metropolia

Tekijä(t) Otsikko Sivumäärä	Ilari Kontio Yritysverkon toteutus 29 sivua
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja(t)	Yliopettaja, Janne Salonen

Työn tarkoitus on toimittaa toimiva tietoverkkoratkaisu Medius Oy:lle. Opinnäytetyössäni suunnittelin ja rakensin yritysverkon hammaslääkäriklinikalle. Verkkoon kuului lähiverkko, langaton lähiverkko sekä laitteisto- ja ohjelmistoasennukset. Verkko kattoi kaikki yrityksen laitteet mukaan lukien hammaslääkärituolit. Tietokoneita verkossa oli 16 kappaletta, tuoleja 5 kappaletta ja palvelinkoneita 3 kappaletta.

Työssä käydään läpi laitteiston suunnittelu, hankinta ja rakentaminen. Tärkeässä osassa on myös tietoturva. Käyn myös läpi varmuuskopioinnin. Palomuurina ja pääreitittimenä käytettiin Cisco ASA -5505 reititintä. Pääkäyttöjärjestelmänä koneissa toimi Windows 7 Professional. Asennukset toteutettiin kaikki paikanpäällä.

Valmiissa ratkaisussa ei ilmennyt mitään odottamattomia ongelmia. Suurin ongelma, mihin törmäsimme, oli riittämätön lisenssi pääreitittimeen. Aikaa ongelmien korjaamiselle varasimme kaksi kuukautta, joka riitti juuri ja juuri.

Hyvä suunnittelu on ehdottomasti suositeltavaa jopa tämän kokoiselle projektille. Säästimme aikaa ja rahaa tekemällä mittavan suunnittelutyön.

Lopputuloksena oli käyttäjäystävällinen ja turvallinen yritysverkko. Verkko suunniteltiin myös helpoksi laajentaa, joten yrityksen verkko- ja ATK-tarpeet saavutettiin hyvin.

Avainsanat	yritysverkko, lääkintä, lähiverkko, langaton lähiverkko, tietoturva

Author(s) Title Number of Pages	Ilari Kontio Corporate network implementation 29 pages
Degree	Bachelor of Engineering
Degree Programme	information technology
Specialisation option	information networks
Instructor(s)	Senior Lecturer, Janne Salonen

The purpose of this work is to provide an effective network solution for Medius OY. In my thesis I designed and implemented the enterprise network for a dentist's clinic. The network consisted of a local area network, wireless local area network, as well as hardware and software installations. The network covered all of the company's equipment, including dental chairs. The clinic had 16 workstations, 5 dental chairs and 3 servers.

The thesis examines the design, procurement and construction of hardware and software. I also cover information security and go through the backup process. Cisco ASA 5505 router was used as a firewall and as the main router. Windows 7 Professional was used as the main operation system. All installation was made at the grounds.

The finished product didn't have any unexpected problems. The main problem which we encountered was insufficient license for the main router. We booked two months for troubleshooting.

Good design is definitely recommended even for this size of a project. We saved time and money by doing it well.

Keywords	enterprise network, medical, LAN, wireless LAN, security

Sisällys

Lyhenteet

ORM	Object-relational mapping. Oliomallin mukaisen esityksen kuvaus relaatiomallin mukaiseksi esitykseksi.
TKHJ	Tietokannan hallintajärjestelmä. Ohjelmisto, jonka avulla hallinnoidaan tietokantoja.

1 Johdanto

Medius Oy on perustettu vuonna 1979 Porvoossa. Tällöin yrityksessä toimi yksi hammaslääkäri. Vuonna 1983 Medius muutti suurempiin tiloihin ja lisäsi henkilöstöään. Näissä tiloissa toimi vuosien aikana useita hammaslääkäreitä sekä lääkäri. Medius hankki myös Porvoon ensimmäisen panoraamatomografialaitteen. Ensimmäinen sähköinen potilastietojärjestelmä hankittiin vuonna 1987.

Kuva 1 Hammalääkäriasema Medius

Vuonna 2002 tapahtui seuraava muutto vanhojen tilojen jäätyä pieniksi. Medius siirtyi Porvoon Lääkärikeskuksen kanssa uusiin tilohin. Tällöin yrityksessä toimi jo leukakirurgian erikoislääkäri. Näihin aikoihin kaikki röntgentutkimukset muutuivat digitaaliseksi ja muutamia vuosia myöhemmin otettiin Promax 3D -laite käyttöön. Promax on KKTT-kuvauslaite eli laite, joka ottaa kolmiulotteisia leikekuvauksia.

Nämäkin tilat jäivät pieniksi, ja niinpä vuonna 2013 syksyllä Medius ja Porvoon Lääkäriasema muuttivat vielä suurempiin tiloihin. Näissä tiloissa Mediuksessa työskentelee

kymmenkunta hammaslääkäriä, muutamia leukakirurgian erikoislääkäreitä sekä kaksi suuhygienistiä.

Opinnäytetyöni on näiden uusimpien tilojen ATK-laitteiden suunnittelu ja toteutus. Aikaa tähän oli varattu vuoden 2013 keväästä vuoden 2013 talveen. Järjestelmän tulisi toimia viimeistään uusien tilojen käyttöönottoon mennessä, eli vuoden 2013 lokakuussa. Tämän jälkeen olisi muutama kuukausi viimeisten vikojen karsimiselle sekä mahdollisten uusien laitehankintojen suunnittelulle.

Systeemin piti kattaa kaksi tietokonetta joka hoitohuoneeseen, yksi tietokone leikkaussaliin sekä yksi tai kaksi tietokonetta potilaiden vastaanottoon. Tämän lisäksi yritykseen tuli erillisiä serverikoneita, jotka pitävät sisällään potilastietokannan, sekä röntgen-ohjelman.

Verkon pitää toimia siten, että muutamalla työntekijällä on pääsy VPN-yhteyden kautta yrityksen intranetiin. Lisäksi yrityksenasiakkailla pitää olla erillinen langaton pääsy Internetiin. Vaatimuksena on myös, että joka kone on verkossa.

2 Teoria

2.1 Laitteisto

Koko systeemin sydämessä on laitteisto. Ilman tätä se ei yksinkertaisesti ole olemassa. Laitteistoon tämän kokoisessa yrityksessä on tietokoneita, tulostimia, reitittimiä ja kytkimiä sekä tietenkin hammaslääkärin tuoleja. Ei toki saa unohtaa suurta määrää hallintalaitteita eli hiiriä, näppäimistöjä ja ehkä mahdollisesti jopa verkkokameroita. Jotta kaikki sujuisi siis sulavasti ja ilman turhia vaikeuksia, laitteiston pitäisi olla myös oikea suunniteltuun tarkoitukseen.

Ensimmäinen pohdittava asia on laitteiston käyttötarkoituksen suunnittelu. 3-D mallintaminen tarvitsee ihan eri pelit kuin raskainkaan tekstinkäsittely. Hinta, virrankulutus ja hallittavuus ovat avainsanoja.

Tekstinkäsittelyyn tarvittavan koneen vaatimukset eivät ole suuret. Tähän riittää kone, joka lähinnä pystyy pyörittämään valittua käyttöjärjestelmää. Ei tarvita kallista näytönohjainta eikä suurta määrää keskusmuistia. Kaikesta voi siis käytännössä valita edullisimman vaihtoehdon. Näitä koneita tulee olemaan aina eniten. Tehokkaat ja kalliit koneet tulee hankkia vain, jos niitä todella tarvitaan. Eikä kaikilla tarvitsevilla tarvitse omaa olla, jos sitä ei käytä koko työpäivää.

Näytöt hammaslääkäriasemalla ovat tärkeässä roolissa. Potilaista otetaan päivittäin röntgenkuvia ja näissä kontrastit ovat tärkeitä. Kontrastien avulla saadaan selville, missä esimerkiksi reiät ja muut suun viat oleilevat. Tähän tarkoitukseen tarvitaan korkeaa tarkkuutta, sekä näyttöjen kalibrointia. Nämä näytöt ovat kalliita, joten on tarkkaan harkittava, kuinka monta näitä oikein tarvitaan.

Näyttöjä saa joko valmiiksi kalibroituna, jolloin hinta nousee entisestään tai sitten ne voi kalibroida itse. Harmaan sävyt ovat tärkeimpiä lääkintätarkoituksessa. Windows 7:stä löytyy sisäänrakennettuna kalibrointisovellus, mutta suositeltavaa tässä tapauksessa on käyttää kolmannen osapuolen kalibrointiohjelmistoa ja laitetta.

Tulostimia on moneen lähtöön perusmatriisikirjoittimesta kolossaaliseen 3-D-tulostimeen. Mediuksen käyttötarkoitukseen tosin riittänee joka lasertulostin- tai mustesuihkutulostinlauma.

Lääkintäalalla puhtaus on kaikki kaikessa. Tämän vuoksi hallintalaitteilta vaaditaan aika paljon. Niiden pitää olla äärimmäisen helppoja puhdistaa ja disinfektoida. Näppäimistöjen on myös hyvä olla litteitä, jotta likaa ei pääsisi vaikeasti puhdistettaviin rakosiin. Kuvassa 2 on huoneen hammaslääkärin työpiste.

Kuva 2 Typillinen hammaslääkärin työasema

2.2 Verkko

Verkko yhdistää systeemin ja saa sen toimimaan kokonaisuutena. Tunnusmerkkinä hyvälle verkolle on se, että kaikkea pystyy hallitsemaan työpisteeltään tuntemattaan olevansa verkossa. Elintärkeää on, että ulkopuoliset eivät pääse käsiksi mihinkään kriittiseen.

Tyypillisen pienyritysverkon sydän on pääreititin. Se reitittää ja estää yhteyksiä tarpeen mukaan. Se ei kaatuile kesällä eikä talvella. Siihen pitää pystyä luottamaan. Tähän laitteeseen siis kannattaa investoida. Reitittimen toiminta seuraavassa, hieno analogia on referoitu wikipediasta (1):

Reititin on kuin maantieverkon tienristeys. Eli ohjaa liikennettä tarvittavaan suuntaan. Kuten teiden, niin myös reitittimien varrella on opasteita, joilla voidaan ohjailla liikennettä kohdettaan kohti laajemmalla kaistalla. Toisin kuin reititin, niin kytkin palvelee yhdentien varrella asuvia asukkaita.

Jotta reitittäminen toimisi, niin reitittimellä tulee olla tieto verkon topologiasta. Topologia mahdollistaa optimaalisimman reititysvalinnan. Reitittimet saavat topologiatietoa sekä reititysprotokollista että ihmisavusteisesti. Kun lähde- ja kohdeverkkojen välille on useita reittejä, reitittimen tehtävänä on valita paras reitti. Reittivalinta voi perustua reitin minimipituuteen, reitin nopeuteen, reiteille annettuihin prioriteetteihin ja niin edelleen. Reittivalinnan perusteita kutsutaan metriikaksi. Reitittimet toimivat OSI-mallin verkkokerroksella (kerros 3).

Yleisin ja yksinkertaisin reititinmalli on kuluttajan ja palveluntarjoajan välissä oleva DSL-modeemi. Laite tuntee sekä oman lähiverkkonsa, että seuraavan hypyn Internetin suuntaan. Käytännössä tämä tarkoittaa sitä, että kun reititin saa paketin, se reitittää sen kohti ainoaa tuntemaansa reittiä.

Monimutkaisemmassa tapauksessa reititin on yhteydessä moniin eri verkkoihin, joista on yhteyksiä vielä kymmeniin muihin verkkoihin. Tämän takia verkkojen osille voi muodostua useita reittivaihtoehtoja, jolloin reititin valitsee parhaan reitin oman tietämyksensä perusteella. Näissä tapauksissa reitittimet käyttävät reititysprotokollia, joiden avulla reitittimet vaihtavat itsenäisesti keskenään reititys- ja metriikkatietoja.

Pääreitittimessä harvoin on kymmeniä portteja, joten seuraava askel on kytkin tai kytkimet. Pääkytkimeksi kannattaa myös valita luotettava laite ja tietenkin tarkistaa, että laite toimii 1Gbit nopeuksilla. Kytkin wikipediasta referoidulla tavalla (2.):

Kytkin yhdistää pakettikytkentäisiä verkon osia toiseensa, jotta saadaan muodostettua yhtenäinen OSI-viitemallin kerroksella kaksi toimiva verkko.

Kytkin tallentaa paketin lähettäjän MAC-osoitteen ja portin kytkimen osoitetauluun. Seuraavaksi kytkin vertaa paketissa olevaa vastaanottajan MAC-osoitetta osoitetauluun ja lähettää paketin eteenpäin oikeaan porttiin. Jos vastaanottajan osoitetta ei löydy taulusta, tai kyseessä on yleislähetys- tai ryhmälähetys-paketti, kytkin lähettää paketin kaikkiin portteihin. Jos vastaanottajan portti on sama kuin lähettäjän portti, paketti hävitetään.

2.3 Langaton Verkko

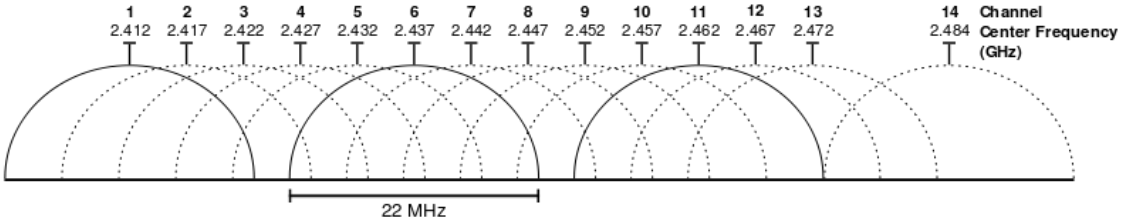
Langaton verkko eli WLAN (wireless local area network) on verkko, joka yhdistää yhden tai useamman laitteen toisiinsa langattomasti, joko suoraan tai tukiaseman kautta. Useimmat uudet WLANit perustuvat IEE802.11-standardeihin. Tällä hetkellä suosituimmat standardit ovat 802.11b (11Mbps) ja 802.11g (54Mbps).

802.11b toimii 2,4Ghz:n alueella, ja nimellinen nopeus sillä on 11 megabittiä sekunnissa. Se on jatkoa standardille 802.11, joka kävi ajan myötä liian hitaaksi. Tiedonsiirrossa standardi käyttää CCK-tekniikkaa (complement code keying). Tämä tarkoittaa, että tieto lähetetään 64:n 8-bittisen koodisanan sarjoina. Sarjamuodossa kullakin koodisanalla on oma matemaattinen merkityksensä. Vaihtoehtoisena siirtotekniikkana 802.11b tarjoaa PBCC-tekniikan (packet binary convolutional coding) ja tukee edeltäjänsä siirtotekniikkaa.

802.11g toimii 2,4Ghz:n alueella ja nimellinen nopeus sillä on 54 megabittiä sekunnissa. Standardi on jatkoa 802.11a:lle. Muutoksia 11a:n nähden on se, että 11g on täysin yhteensopiva 11b:n kanssa. 802.11a toimitaajuusalue oli myös eri, eli 5Ghz:n alue.

Mediuksen verkko laitettiin toimimaan 2.4 GHz:n alueella. Tämä loi lisää haasteita, koska kaikki lähellä sijaitsevat verkot toimivat myös tällä alueella. 2.4 GHz:n kanavia on Suomessa käytössä kolmetoista. Muualla maailmassa niin kuin esimerkiksi Yhdysvalloissa

sallittuja kanavia on vain yksitoista. Vaikka kanavia onkin kolmetoista käytössä, niin tästä määrästä vain kanavat 1,6 ja 11 eivät mene toistensa päälle. Kanavat toimivat tietyillä 22MHz:n alueilla, joten esimerkiksi kanavat yksi ja kaksi menevät päällekkäin todella pahasti taajuusalueillaan. Kun yhdellä taajuusalueella on käyttöä, joutuvat muut aluetta käyttävät odottelemaan omaa vuoroaan. Seurauksena tästä on se, että kaikkien verkon käyttö hidastuu.



Kuva 3 2,4 GHz kuuluvuusalueen kanavat

Maailmassa on useita eri protokollia langattoman liikenteen suojaamiselle. Seuraavassa muutamia yleisiä tekniikoita.

WEP on alkuperäinen WLAN-tekniikan salausprotokolla. Se on vanha ja verkkohyökkäyksille altis. WEP käyttää 40-, 104- tai 232-bittistä salausta, mutta sen RC4-salausprotokollassa olevan puutteen vuoksi joidenkin pakettien kehyksissä lähetetään salaamattomia bittejä, alustusvektoreita ja niiden perusteella voidaan helposti laskea käytetty salausavain.

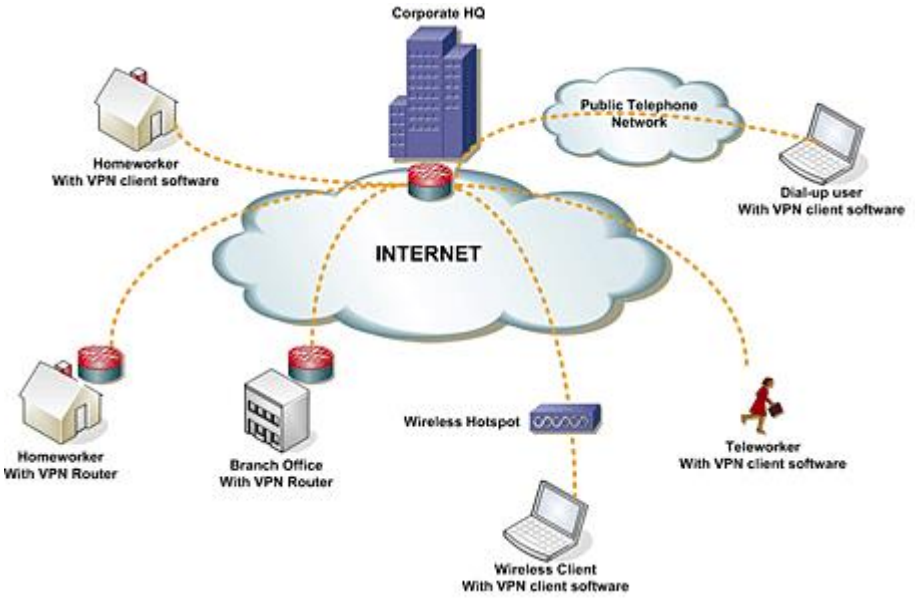
WPA:n uudempi salausmetodi poistaa WEP-salauksen tunnetut ongelmakohdat. Lähinnä staattisesta salausavaimesta johtuvat. TKIP käyttää 128-bittistä pakettikohtaista salausavainta tukiaseman ja asiakkaan välisessä liikenteessä. WPA-salaus sisältää myös pakettien eheyttä valvovaln MIC (Message Integrity Check) -toiminnon. Tämä tarkistaa jokaisen paketin, jolloin hyökkääjä ei pysty kaappaamaan ja muuttamaan pakettien tietoja.

AESia vastaan ei ole yhtään tunnustettua hyökkäystä. Kaikki AESia käyttävät tekniikat on hyväksytty salaamaan Yhdysvaltojen hallituksen "non-classified" -luokiteltu tieto Kansallisen turvallisuusviraston (NSA) puolesta. Tämä on ensimmäinen kerta, kun siviileillä

on pääsy salaustekniikkaan, jonka NSA on hyväksynyt salaamaan TOP SECRET -luokittelemaansa aineistoa.

2.4 VPN

VPN (Virtual private network) on tekniikka, jolla voidaan yhdistää useampi yksittäinen verkko julkisen verkon yli muodostaen näennäisesti yhden yksityisen verkon pisteiden välille. VPN-määritelmää on jouduttu laajentamaan käsittämään myös yksittäisten tietokoneiden ja laitteiden liittämisen yrityksen verkkoon etätyöskentelyn suosion kasvaessa. VPN-verkko voidaan toteuttaa joko reitittimien, palomuurien tai VPN-palvelinohjelmistojen avulla (3). Alla kuva erilaisista VPN-yhteysmuodoista.



Kuva 4. Erilaisia VPN-yhteysmuotoja

Ensimmäinen toteutusvaihtoehto on käyttää reitittimiä yksinään VPN-yhteyden luomiseen (router-to-router VPN). Tämä tarkoittaa yksinkertaisesti sitä, että reitittimet hoitavat tiedon kryptauksen ja avauksen itsenäisesti, jolloin säästytään erillisen laitteiston ostamisesta näihin tehtäviin.

Tästä toteutustavasta löytyy kuitenkin myös monenlaisia ongelmia. Reititin voi esimerkiksi olla jo niin suuren kuorman alla, että koko verkon toiminta hidastuu kun lisätään reitittimen vastuulle myös VPN. Tämä vaihtoehto myös aiheuttaa riippuvuuden yhteen reititinvalmistajaan, koska ratkaisut eri reitittimien välillä eivät ole yhteensopivia. Tämän lisäksi tietoturvan ja kaiken muunkin tekniikan kehityksessä joudutaan odottamaan päivityksiä reititinvalmistajalta.

Toinen vaihtoehtoinen toteutustapa on luoda VPN-etäyhteys (VPN remote access). Tämä perustuu verkkoon asennettuun erilliseen tietokoneeseen, joka valvoo liikennettä ja hoitaa salauksen ennen kuin data kulkeutuu reitittimelle. Sama tapahtuu myös käänteisessä tapauksessa, kun data saapuu verkkoon. Ensin tietokone purkaa datan, ja sitten se kulkeutuu reitittimelle, joka laittaa sen eteenpäin.

Tässä toteutustekniikassa on monia hyviä puolia. Missään vaiheessa ei olla riippuvaisia yhdestä reititinvalmistajasta, ja tietoturvallisuus on samaa tasoa, ellei jopa parempi kuin käytettäessä pelkkiä reitittimiä. Näiden lisäksi mahdollisten liikkuvien käyttäjien lisääminen VPN palveluun on helpompaa.(4).

2.4.1 IPsec

IPsec on alun perin IPv6:lle kehitetty kolmannen tason protokolla, jonka tarkoitus on varmistaa päästä päähän -salaus verkossa siirrettävälle tiedolle. Se tarjoaa samalla pääsynhallinnan, vuon eheyden ja lähteen varmistuksen sekä suojan liikenteen toistamiselta myös ylempien OSI-mallin verkkosovelluksille. Käytännössä IPsec käyttää kahta protokollaa, IP Authentication -kehystä (AH) ja ESP:ta liikenteen autentikointiin ja salaukseen. Lisäksi tarvitaan turvalliset käytännöt avainten hallintaan ja vaihtamiseen yhteyspisteiden välillä.

IPsec-protokollaa voidaan käyttää VPN-ratkaisuna kahdella eri tavalla. IPsec:n luoman tunnelin salauksessa jolloin koneiden tai jopa koko lähiverkon liikenne ohjataan erilliseen laitteeseen, kuten palomuurin. Laite hoitaa liikenteen salauksen ja paluuliikenteen purkamisen. Tämä ratkaisu on hyvä silloin, kun tiedetään vastaanottavan ja lähettävän verkon olevan turvallisia.

Toinen vaihtoehto on turvata liikenne koko matkalta lähettäjältä vastaanottajalle siten, että tietokoneet itse hoitavat kaiken salaukseen vaativan prosessoinnin. Hyvänä puolena tässä vaihtoehdossa edelliseen verrattuna on, että data ei missään vaiheessa ole salaamaton. Vaikka joku onnistuisi pääsemään verkkoon käsiksi, niin data olisi yhä suojattu kolmannelta taholta.

Ainoana heikkoutena IPseci:ssä voidaan mainita, että standardissa ei ole mitenkään määritelty IP-osoitteiden hallintaa. Jos käyttäjä haluaa ottaa etäyhteyden, niin IP-osoiteasetukset ja muut asetukset tulee olla staattisesti ennalta konfiguroitu. Tämä ongelma on kyllä ratkaistu jo, mutta sitä ei käytetä vielä missään tuotteissa. Yleisimpänä ratkaisuna tällä hetkellä on valmistajakohtaiset ratkaisut, jotka aiheuttavat aikaisemmin mainitut ongelmat eri valmistajien laitteiden käyttämisestä VPN:ää luodessa. (5.)

2.4.2 Avoimen lähdekoodin VPN-sovellukset

Parhaat puolet avoimen lähdekoodin sovelluksissa on, että ne ovat ilmaisia ja erittäin turvallisia. Esimerkiksi Free S/Wan VPN tai OpenBSD VPN tarjoaa yhtä hyvän suojan kuin maksulliset ohjelmistot. Näissä vaihtoehdoissa tulee olla valmis toimimaan Linux- tai OpenBSD-käyttöjärjestelmillä.

Huonoja puolia taas verrattuna kaupallisiin ratkaisuihin on käyttötuen kaaos. Toisin kuin kaupallisilla ratkaisuilla, ilmaisilla ohjelmilla ei ole keskitettyä tukea vianselvitykseen tai valmiita ratkaisuja selkeästi jäsennettynä. Yleensä näitä ohjelmia käyttäessä tulee apua etsiä foorumeilta ja toisilta käyttäjiltä, mikä tarkoittaa mahdollisten ongelmien hitaampaa ratkaisua. (6.)

2.5 Ohjelmisto

Ensimmäinen tärkeä ohjelmistovalinta on käyttöjärjestelmä. Niitä on monia erilaisia moneen eri käyttöön. Käyttöjärjestelmän valintaan vaikuttaa se, mitä ohjelmia sillä aiotaan käyttää.

Käyttöjärjestelmän tehtäviin kuuluu laitteiston hallinta, tiedostojärjestelmä, muistinhallinta, virtuaalimuisti, prosessienhallinta, verkkoprotokollat ja käyttäjät eli siis kaikki, jotka

saavat tietokoneet toimimaan. Se toimii myös rajapintana ihmisen ja koneen välillä. Käyttöjärjestelmä koostuu seuraavista tärkeistä ominaisuusksista.

- laitteiston hallinta, komponenttien ja ohjelmistojen välille tarjottu yhteinen rajapinta.
- tiedostojärjestelmä, tapa jolla käyttöjärjestelmä hallitsee tietoa
- muistinhallinta, tarjoaa prosesseille häiriövapaan muistialueen
- virtuaalimuisti, varamuisti keskusmuistin loppuessa
- prosessienhallinta, hallitsee prosesseja ja niiden muistinkäyttöä
- verkkoprotokollat, OSI-mallin 3. ja 4. tason hallinta
- käyttäjät, käyttäjien oikeuksien hallinta

Mediuksessa on ms-dos:in jälkeen käytetty Windows-käyttöjärjestelmiä. Kaikki työhön tarvittavat sovellukset toimivat myös Microsoftin järjestelmissä, joten päätimme vertailla eri Windows-versioita ja valita niistä toimivimman yrityksen tarkoitukseen.

Käyttöjärjestelmäksi valittiin loppujen lopuksi Windows 7. Windowsista on kolme eri versiota Home Premium, Professional sekä Ultimate. Näistä kolmesta päätimme ottaa Windows 7 professionalin. Kuvassa 5 on vielä Windows 7 -käyttöjärjestelmien eroja.

Kuva 5. Windows 7 –käyttöjärjestelmien erot

Ohjelmat pyrittiin pitämään mahdollisimmanautomatisoituina, jotta käyttäjät eivät joudu ongelmiin visaisten päivitysvalintojen kanssa. Ohjelmamäärät pyritään myös pitämään kurissa, sillä mitä enemmän ohjelmia sen enemmän ongelmia. Pahimpia ovat yhteensopivuusongelmat, joita pyrittiin välttämään.

2.6 Varmuuskopiointi

Varmuuskopiointi on tapa säilyttää tietoa. Tieto kopioidaan useaan eri paikkaan, jolloin ongelmien tapahtuessa tieto on silti käytettävissä. Tällaisiä ongelmia ovat käyttäjän poistama väärä tiedosto tai kiintolevyn rikkoontuminen. Lisäksi varkaus tai tulipalo voi tulla kyseeseen.

Varmuuskopionti on suoritettava suhteellisen usein, jotta tieto ei pääse vanhentumaan. On myös syytä pitää huoli, että varmuuskopioita on useita, sillä ikuista tallennusvälinettä ei ole olemassa.

Kopioita ei kannata ottaa kaikista tiedostoista. Windows 7 osaa itse tehdä palautuspisteitä, joten työasemien käyttöjärjestelmistä on turha ottaa varmuuskopioita. Jos käyttöjärjestelmä jostain syystä sekoaa, sen voi useissa tapauksissa palauttaa aikaisempaan ajankohtaan. Operaatio ei myöskään vie hirveästi aikaa. Tietokannoista tulee ottaa varmuuskopiot. Nämä muuttuvat usein ja sisältävät elintärkeää tietoa. Tietokannan hävitessä sitä on mahdoton palauttaa.

Terveydenhuoltoyrityksellä on tiedot potilaistaan, jotka eivät saisi missään nimessä hävitä, eikä niitä myöskään saisi varastaa. Tämän vuoksi suunnittelimme, että otamme varmuuskopioita muutamalla eri tavalla.

Ensimmäinen tapa on lähinnä konevian hallintaa. Ajattelimme, että peilaamme alkuperäisen kovalevyn RAID1-tekniikalla. Tämä tarkoittaa sitä, että koneeseen tulee vähintään kaksi kovalevyä. Näihin levyihin tallennetaan sama data, jolloin jos yksi levyistä hajoaa, säilyy tieto vielä muilla levyillä. RAID1 myös periaatteessa nostaa lukunopeutta, koska järjestelmä voi lukea usealta levyltä dataa samanaikaisesti (7).

Toinen tapa on kerran päivässä tapahtuva varmuuskopiointi verkkolevylle. NAS (network-attached storage) on tallennusjärjestelmä, joka kytketään suoraan verkkoon. Se sisältää sulautetun palvelimen ja yhden tai useamman kiintolevyn.

Kolmas ja viimeinen tapa on verkon yli tapahtuva varmuuskopiointi. Tämä todennäköisesti tulee olemaan NAS-järjestelmä, joka sijoitetaan turvalliseen paikkaan. Internet-yhteyden NAS-järjestelmälle tulee olla riittävän nopea ja luotettava. Tämä varmuuskopiointi suoritetaan kerran viikossa.

Tietokannat tulee kryptata, jotta varastetulla levyllä ei voida tehdä mitään. Se kuitenkin alentaa suorituskykyä ja nostaa kustannuksia. Kryptausohjelmia on useita mm. Microsoftin oma BitLocker. Tämä ei kuitenkaan sisälly Windows 7 Professionaliin.

3 Tietoturva

Tietoturvalla tarkoitetaan tietojen väärinkäytön estämistä. Se koostuu eheydestä, käytettävyydestä ja luotettavuudesta.

Luottamuksellisuudella tarkoitetaan sitä, että tiedot, järjestelmät ja palvelut ovat vain niihin oikeutettujen saatavissa eikä niitä luvatta paljasteta tai muutoin saateta sivullisten tietoon.

Eheydellä tarkoitetaan sitä, etteivät tiedot, järjestelmät tai palvelut ole laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet.

Käytettävyydellä tarkoitetaan sitä, että tiedot, järjestelmät ja palvelut ovat tarvittaessa niihin oikeutettujen esteettä hyödynnettävissä.

Tietoturva on usein käyttäjästä kiinni. Käyttäjätunnusten määritteleminen on hyvä tehdä etukäteen. Kaikki käyttäjät eivät taatusti tarvitse järjestelmän valvojan oikeuksia. Normikäyttäjälle riittää, kun pystyy käyttämään valmiiksi asennettuja ohjelmia ja tallentamaan töitänsä. Täten myös riittää, että käyttäjä pääsee vain omaan kotihakemistoonsa.

Hyvä salasana on tärkeä turvallisuustekijä. Se ei saa olla liian lyhyt, eikä toisaalta liian helppo. Yleisin salasana on lähiaikoina ollut ”123456” (8.). Käytettävän salasanan tulisi olla vähintään 8-merkkinen, jossa on isoja ja pieniä merkkejä. Eikä se mielellään saisi olla mikään, ainakaan englanninkielinen, sana.

Tietokoneille eivät ulkopuoliset saa päästä käsiksi. Huoneet, joissa on koneita, on pidettävä lukittuna, kun siellä ei ole ketään. Erityisesti palvelinkoneille ei asiattomien ihmisten tule päästä. Henkilökunnan on myös ymmärrettävä, että salasanoja pitää käsitellä erittäin huolellisesti. Niitä ei saa kirjoittaa lapuille ja jättää lojumaan.

Maailman ensimmäisenä tietokoneviruksena pidetään vuonna 1982 kirjoitettua Elk Cloner -nimistä ohjelmaa. Toisin kuin nykyvirukset, jotka leviävät kulovalkean tavoin internetissä, tämä levisi Apple II -tietokoneisiin levykkeillä. Ensimmäinen tunnettu PC- virus on vuodelta 1986 nimeltään (c)Brain. Nämä virukset eivät olleet haitallisia, esimerkiksi (c)Brain muutti kiintolevyn nimeksi (c)Brain.

Viruksiin kuuluu kolme alalohkoa: itse virukset, madot ja troijalaiset. Perusvirukset ovat haittaohjelmia, jotka kopioituvat ohjelmien ja verkkoyhteyksien kautta. Niiden tarkoitus on vahingoittaa tietokonetta sekä vaikeuttaa sillä työskentelyä. Ne eivät leviä itsekseen vaan vaativat, että saastunut tiedosto joko suoritetaan tai avataan.

Madot ovat ohjelmia, jotka leviävät ohjelmien tietoturva-aukkojen kautta. Ne tulevat aukoista sisään ja kopioituvat ilman, että käyttäjä suorittaa saastuneita tiedostoja. Luonteeltaan ne ovat samanlaisia kuin perinteiset viruksetkin.

Troijalaiset ovat viattoman näköisiä ohjelmia. Ne näyttävät tekevän jotain hyödyllistä, mutta avaavatkin samalla haavoittuvuuden tietojärjestelmässä. Näiltä on kuitenkin helppo suojautua. Ei tule koskaan avata ohjelmaa, jonka alkuperästä ei voi olla varma.

Vakoiluohjelmat ovat yleensä vähintäänkin yhtä vaarallisia kuin virukset. Ne eivät sekoita käyttöjärjestelmää samalla tavalla, mutta ne saattavat kerätä esimerkiksi tietoja käyttäjästä tai tietokoneesta. Yksi yleisimmistä vakoiluohjelmatyypeistä on keylogger, jolla yleensä varastetaan käyttäjän naputtelemat käyttäjätunnukset ja salasanat.

Virukset ja haittaohjelma ovat vakava tietoturvauhka. Näitä vastaan koneisiin asennetaan virusturva, palomuuri ja haittaohjelmien esto/poisto-ohjelmat. Virusturvassa ja palomuureissa on paljon valinnanvaraa. Ohjelmien käytettävyydessä ja tehovaatimuksissa on kuitenkin suuria eroja. Vertailimme F-Securen, McAfee, Symantekin ja Aviran tarjoamia ratkaisuja ja hankimme näistä tarpeisiimme sopivimman. Vaatimuksina oli, että ratkaisun pitää olla mahdollisimman automatisoitu, sekä että sen pitää tukea Windows 7 -

käyttöjärjestelmää. Tämän lisäksi olisi suotavaa, että ratkaisu kattaisi koko tietoturvan yksinkertaisuuden takia.

Microsoftilla on myös oma tietoturvaohjelmisto nimeltään Microsoft Security Essentials. Se ei tule Windows 7:n mukana, mutta on vapaasti ja ennen kaikkea ilmaisesti ladattavana käyttöjärjestelmän omistajalle. Tämän käyttöä emme vakavasti harkinneet, mutta kävimme sen silti läpi.

Omien selvitysten lisäksi tutustuimme AV-Comparatives-testauslaboratorion tietoturvatuloksiin. AV-Comparatives on itävaltalainen virusturvan testauslaboratorio. Se julkaisee tuloksiaan säännöllisesti Internetissä. Järjestö on voittoa tavoittelematon, ja sen rahoitus tulee tietoturvayhtiöiltä, jotka haluavat tuotteensa testeihin. Lisärahoitus tulee yliopistoilta ja muilta akateemisilta tahoilta. Järjestön kotisivut löytyvät osoitteesta http://www.av-comparatives.org/.

3.1 F-secure

F-securen tarjoaman ratkaisun nimi oli ”F-Secure Protection Service” (PSB). Se on kaikenkattava tietoturvaratkaisu. Paketti sisältää virusten ja vakoiluohjelmien torjunnan, palomuurin, rootkit-ohjelmien tunnistuksen, roskapostineston sekä nopean suojauksen uusilta tuntemattomilta uhilta. Tarjotun palvelun isännöinnistä ja hallinnoinnista vastaisi paikallinen IT-kumppani. Eli käytännössä F-secure tarjoaisi hallintainfrastruktuurin. Tämä olisi siinä mielessä hyvä asia, koska Mediuksella on järjestelmän asennuksen jälkeen rajoitettu määrä IT-henkilökuntaa. Paketti toimisi myös Windows 7 -koneilla, sekä Mac OS:llä, jos niitä yritykseen myöhemmin hankittaisiin.

F-Secure Protection Service pitää sisällään myös muutamia F-Securen omia teknologioita. Ne ovat nimeltään DeepGuard, BlackLight ja Software Updater

DeepGuard on F-Securen kehittämä teknologia, joka analysoi tiedostojen sisältöä ja ohjelmien toimintaa ja estää uudet sekä vielä määrittelemättömät virukset, madot ja muut haitalliset ohjelmat, jotka yrittävät tehdä mahdollisesti haitallisia muutoksia tietokoneeseen. Periaatteessa tämä kuulostaa hyvältä, mutta käytännössä on olemassa le-

gittejä ohjelmia, jotka tekevät muutoksia koneelle, jonka takia DeepGuard estää kyseisen muutoksen. Tämän saa kuitenkin kierrettyä sillä, että asennuksen jälkeen lisätään tarvittavat ohjelmat DeepGuardin-poikkeuslistalle.

Blacklight tunnistaa rootkit-ohjelmia. Rootkit-ohjelma on eräänlainen takaovi tietokoneeseen. Se asentuu tietokoneeseen normaalisti tietoturva-aukon kautta ja pyrkii piilottamaan itsensä sekä vieraat prosessit mahdollisimman hyvin. Tämän jälkeen hyökkääjä saa normaalisti järjestelmänvalvojan oikeudet saastuneeseen koneeseen. Blacklight käy tietokoneen kansiot, tiedostot ja piilotetut prosessit läpi. Tämän jälkeen ohjelma listaa mahdolliset tartunnat. Pitää kuitenkin pitää mielessä, että kaikki epäilykset eivät ole tartuntoja, vaan jokainen tapaus pitää käsitellä tarkasti. Esimerkiksi, jos prosessin tekijä on Microsoft Corporation, ei välttämättä ole hyvä idea poistaa kyseistä prosessia.

Software Updater -ohjelmistopäivitys ohjelmiston voi ohjelmoida päivittämään melkein minkä tahansa kolmannen osapuolen ohjelmiston, mukaan lukien Windowsin omat päivitykset.

3.2 Symantec

Symantec tarjoaa suuren määrän palveluita, mutta se, johon me päädyimme oli Symantec Endpoint Protection. Paketti pitää sisällään virusten torjuntaohjelmiston, palomuurin sekä rootkit-ohjelmien tunnistuksen. Symantecin maailamlaajuisen verkoston ansiosta jokaista tiedostoa ei tarvitse käydä läpi. Syy tähän on se, että turvalliset tiedostot, jotka löytyvät Symantecin tietokannasta, ohitetaan skannauksen yhteydessä, jolloin säästetään aikaa. Ratkaisu täytti vaaditut vaatimukset, eli toimimisen Windows 7 -ympäristössä.

Symantec Endpoint Protectionissa on pilvessä toimiva ohjelmisto, jonka kautta lisätään haluttuja työasemia suojauksen piiriin. Ratkaisu on yksinkertainen, koska kaikki asetukset voidaan hoitaa pilvipalvelun kautta, jolloin yksittäisillä työasemilla ei tarvitse tehdä mitään.

Niin kuin F-Securessa, myös Symantecilla on omia teknologioita integroituna palveluun. Näistä suurimmat ovat Insight ja SONAR.

Insight on pilvi-pohjaineneknologia, joka tunnistaa uusia ja mutatoituneita uhkia. Tunnistukseen se käyttää tiedoston ikää, toistumista, olinpaikkaa sekä anonyymia telemetriadataa.

Symantec Online Network for Advanced Responce (SONAR) tunnistaa uhkia niiden käyttäytymisen perusteella. SONARIn pääkäyttö on nollapäivähaavoittuvuuksien tunnistaminen.

3.3 Avira

Aviran Business Security Suite on suunnattu yrityksille, joissa on alle 26 työasemaa ja palvelinta. Paketti pitää sisällään perusominaisuudet sekä sähköposti-suodattimen ja anti-adwaren. Muista poiketen ohjelmisto sisältää varmuuskopio-ohjelmiston. Niin kuin muissakin ohjelmissa, nAvirallakin on käytössä heuristinen uhkien tunnistaminen.

Asennus hoidetaan helppokäyttöisen hallintakonsolin kautta. Ohjelmistolla ei voida hallinnoida mobiililaitteita, eikä Applen laitteita. Vaikka ohjelma on yrityksille suunnattu, se pitää sisällään lapsilukkoasetukset.

3.4 McAfee

MCAfeen ohjelmisto on mielikuvituksellisesti nimetty Security for Businekseksi. Tämä pitää sisällään kaikki perustoiminnot, eli virusturvan, palomuurin, sähköpostisuodattimet sekä haittaohjelmien tunnistamisen. Ikävä kyllä kolmannet osapuolet eivät pidä tällä hetkellä McAfeen haittaohjelmien tunnistusta mitenkään hyvänä. Tämän voi kuitenkin ohittaa estämällä pääsy sivuille, jotka ovat vähääkään epäilyttäviä. Tuote toimii Windows 7:llä, joten vaatimukset täyttyvät.

Pilvipohjaista ohjelmistoa hallitaan selainpohjaisen ohjelmiston kautta. Niin kuin Symantecissa, niin myös McAfeessa työasemien säädöt hoidetaan selainpohjaisen hallinnointi konsolin kautta. Ohjelma päivittää itseään tarvittaessa, eikä alkuasentamisen jälkeen tarvitse juurikaan huoltoa.

3.5 Security Essentials

Vaikka Security Essentials on ilmainen, ja se toimii Windows 7 -käyttöjärjestelmässä, niin yrityskäytössä se saa olla asennettuna vain kymmeneen tietokoneeseen. Medius yrityksellä koneita on kuitenkin jo alkutilanteessa 16, niin Security Essentialsin voi unohtaa.

Ohjelmisto sisältää perustoiminnot virusturvan ja haittaohjelmien tunnistamisen. Palomuuri tulee itse käyttöjärjestelmän puolelta. Se on erittäin helppo asentaa eikä vaadi minkäänlaista huoltoa käyttäjän päästä.

4 Käytäntö

4.1 Laitteisto

Yrityksen uusissa tiloissa on hoitohuoneita enemmän kuin vanhoissa, joten päädyimme hankkimaan uudet koneet joka huoneeseen. Vanhoissa tiloissa joka huoneessa oli vain yksi tietokone, mutta totesimme, että hoitotyö olisi nopeampaa, jos hoitajalla olisi oma tietokoneensa. Huoneiden pöytäkoneiksi tuli loppujen lopuksi Acer Veriton M288:t niiden hinta-laatu-suhteen takia. Tietokoneilta ei vaadittu paljoa suoritustehoa, koska niillä oli lähinnä tarkoitus käsitellä tekstiä ja tutkiskella röntgenkuvia.

Vanhoja, toimintakuntoisia koneita siirtyi uusiin tiloihin kuusi kappaletta. Kaksi näistä koneista oli palvelinkoneita, joissa toisessa pyöri potilastietojärjestelmä ja toisessa 3D-kuvauslaskentajärjestelmä.

Muita laitehankintoja olivat kaksi reititintä. Toinen asiakkaiden langattomaan verkkoon ja toinen yrityksen varsinaiseen tietoverkkoon. Asiakasreitittimeksi valitsimme Buffalon Wireless-N-reitittimen sen hyvän ohjelmiston ja luotettavuuden takia. Yritysverkon reitittimeksi valitsimme Ciscon ASA 5505:n.

Kytkimeksi, yrityksen verkkoon valitsemme Hewlett-Packardin 1410-24G 10/100/100 24-porttisen kytkimen. Se on edullinen perusmalli yrityskäyttöön. Kytkintä ei voi hallita, mutta

kyseisessä verkossa se ei haittaa. Lisäksi kytkimiä voi ketjuttaa, sillä kaikki portit tunnistavat kaapeloinnin (MDI/MDI-X).

Uusia tulostimia ei hankittu, vaan vanhat laitteet otettiin käyttöön. Joka hoitohuoneeseen tuli oma tulostin, nämä laitteet olivat kaikki erilaisia ja eri aikoihin hankittuja, pääajatuksena ollen ”vaihdetaan kun hajoaa”. Yksi kyseisistä tulostimista oli niin vanha, että siihen ei löytynyt Windows 7 -ajureita. Tämä laite asennettiin siis Windows XP -koneeseen. Tulostimien lisäksi uusiin tiloihin asennettiin faksi, sekä skanneri potilaiden vastaanottotilaan. Näiden lisäksi hankimme n. 30 kappaletta yhden metrinpituista parikaapelia sekä saman verran kolmen metrin pituisia parikaapeleita.

Lääkintämaailma tarvitsee myös helposti puhdistettavia hallintalaitteita. Tämä siksi, että ihmisten suussa on kasoittain bakteereja ja hammaslääkäreiden työnkuvaan kuuluu sorkkia suita. Mediuksella oli kahden eri valmistajan hallintalaitteita testissä ennen varsinaista ostopäätöstä.

Esterlinen tarjoama Medigenic-näppäimistö on kumipäällysteinen litteä näppäimistö, jonka saa puhdistettua hetkessä. Näppäimistössä on nappi, joka disabloi näppäimistön toiminnan puhdistuksen ajaksi. Se yllättäen kestää kosteutta ja disinfektointiaineita. Näppäimistöön saa myös asennettua puhdistushälytys toiminnon. Tämä pitää huolen siitä, että näppäimistö puhdistetaan säännöllisesti. Näppäimistö on myös valaistu, jolloin sitä voi käyttää hyvinkin pimeässä. Näppäintuntuma oli itsessään olematon, mutta näppäimistön antamat äänimerkit näppäinpainallusten yhteydessä tekivät käyttökokemuksesta hyvän. Hiirestä tosin puuttui rulla, joka vaati totuttelua. Medigenicin näppäimistö ja hiiri kuvattu alla.

Kuva 6 Medigenic-näppäimistö ja hiiri

Cleankeys toimitti toiset testattavat hallintalaitteet eli CK3-17:n. Kuten Medigenic, myös Cleankeys on litteä näppäimistö helposti puhdistettavalla pinnalla. Pinta on valmistettu Gorilla Glass -lasista. CK3-17:n näppäintuntuma on huono, näppäinten vasteajat ovat anteeksiantamattoman pitkät, vaikka siinä on viisi eri herkkyystilaa. Huvittavinta tässä on se, että osa näppäinpainalluksista tuntuu jäävän kokonaan noteeraamatta, jolloin kirjoittaminen muuttui tuskaisaksi. Hiiressä on sentään rulla. Cleankeys-näppäimistön on kuvassa 7.

Kuva 7 Cleankeys-näppäimistö

4.2 Verkko

Tiloissa tarvittiin Internet-yhteys sekä nopea lähiverkko potilastietojen siirtämistä varten. Internet-liittymän oli oltava leveähkö laajakaista. Vanhoissa tiloissa oli Sonera-yrityslaajakaista, jonka siirsimme uuteen osoitteeseen. Kyseisen liittymän mukana tuli neljä dynaamista ulkoista IP-osoitetta ja verkkopalomuuripalomuuri. Tämän lisäksi yrityksellä on käytössä yksi staattinen IP-osoite. Kotisivuja ei tarvitse ylläpitää, koska nämä ovat toisen yrityksen hallinnassa.

Verkkoon suunnittelimme kaksi eri osiota, henkilökunnanverkon ja asiakasverkon. Asiakasverkkoon riitti pelkkä langaton yhteys. Henkilökunnan verkko toteutettiin niin, että vain johdolla pääsee verkkoon. Sisäverkon keskellä on Soneran tarjoama asiakasmodeemi. Tästä jaamme verkon kahteen osaan. Asiakasverkolla on vain pääsy Internetiin, ja sen nopeus on rajoitettu, jotta se ei syö koko yrityksen Internet-kaistaa. Yhteydelle loimme käyttäjätunnukset, jotka asiakkaat saavat odotushuoneesta.

Salauksena käytimme WPA2-personal-salausta (Wi-Fi protected access 2). WPA2:sta on kaksi eri mallia Personal ja Enterprise. Erona näillä on se, että Enterprise käyttää todennuspalvelinta, kun taas Personal käyttää jaettua suojausavainta, koska yritys ei ole kovinkaan suuri niin Personalin käyttö sopii tähän huomattavasti paremmin. Salaus on 128-bittinen, joten se on huomattavan hankala murtaa.

Asiakasmodeemista vedimme parikaapelin yrityksen sisäiseen reitittimeen. Reitittimestä vedettiin parikaapeli 24-porttiseen kytkimeen, jotta joka koneelle riittää piuha. Tästä kytkimestä vedettiin piuha joka koneeseen sekä myös verkkokovalevyille. Jos yritys hankkii lisää tietokoneita tai laitteita, jotka tarvitsevat parikaapelin, voidaan verkkoa laajentaa

Kuva 8 parikaapeli

lisäämällä kytkimiä. Hammaslääkärin tuolit piti myös kytkeä verkkoon, koska joka tuolissa on sisäänrakennettuna Windows XP:llä pyörivä tietokone.

Jokaiseen hoitohuoneeseen sekä aulaan asennettiin myös korttimaksupääte. Jokainen pääte tarvitsi oman langallisen verkkoyhteytensä, joten jouduimme pikaisesti tilaamaan uuden kytkimen, jotta tietoliikenneportit riittivät. Päätteiden asennus oli helpohkoa: teimme niille reiät palomuuriin, jonka jälkeen maksaminen kortilla muuttui mahdolliseksi.

4.3 Reititin

Reitittimeksi valitsimme Cisco ASA 5505:n. Valintaan vaikutti, että olimme koulussa käyneet useita Ciscon kursseja, joten komennot ja toiminta olivat ennestään tuttuja.

Laitteesta löytyvät perusominaisuudet, eli palomuurisuojaus, VPN-tuki ja VLAN-tuki. Tuote on suunniteltu yrityskäyttöön.

Käyttöönotto oli helppoa. Laitoimme virrat päälle ja kävimme asetukset läpi Ciscon graafisella käyttöliittymällä. Kun asetukset olivat mielestämme oikein, kytkimme parikaapeleilla tietokoneet verkkoon. Verkko heräsi henkiin, ja tieto rupesi virtaamaan yrityksen sisällä. Langatonta verkkoa emme laittaneet päälle.

4.4 Langaton verkko

Yrityksen langaton verkko suunniteltiin ainoastaan asiakkaiden käyttöön. Syy tähän oli pääasiassa se, että kaikki henkilökunnan käyttämät verkkolaitteet olivat parikaapelilla kiinni, joten langaton verkko olisi ollut turha ja taas uusi turvallisuusriski.

Reitittimeksi valittiin Buffalon Wireless-N-sarjan reititin. Reitittimeltä ei vaadittu paljoa Siitä piti päästä langattomasti internettiin ja sen tuli sisältää mahdollisuus WPA2-tason suojaukseen.

Langaton verkko analysoitiin iPadiin asennettavalla NetSpot-ohjelmistolla. Ohjelma toimii niin, että kartoitetaan verkon kattama alue,mittaamalla verkon voimakkuuksia halu-

tuilla alueilla. Tämän jälkeen NetSpot luo kuuluvuuskartan, johon ohjelma yrittää paikallistaa Access Pointit parhaansa mukaan. Ohjelma kertoo myös, mille kanavalla mikäkin verkko operoi mittauksen hetkellä.

Sijoitimme langattoman reitittimen odotushuoneeseen. Koko yrityksen alueelle emme saaneet kuuluvuutta yhdellä reitittimellä, mutta eipä tuota verkkoa juuri muilla alueilla tarvittu kuin odotushuoneessa.

Verkon käyttöä oli muutamalla muulla kanavalla kyseisessä paikassa. Teimme uusia mittauksia seuraavina päivinä ja totesimme, että muut Access Pointit oli asetettu valitsemaan kanavan automaattisesti. Tämän seurauksena asetimme reitittimen toimimaan manuaalisesti aina samalla kanavalla, jotta emme aiheuttaisi lisää kanavavaihtelua, kun reitittimet yrittävät löytää epätoivoisesti vapaampaa kanavaa.

Testailimme verkon toimintaa vielä muutamia päiviä. Lopputulos oli se, että verkko toimi tarpeeksi sulavasti ja emmekä tehneet lisää muutoksia.

4.5 Ohjelmisto

Vertailun tuloksena päädyimme siis Windows 7 Professionaliin. Valinta vaikutti suoraan koneiden ostopäätökseen, sillä sen piti sisältää Windows 7 Professional. Vanhoissa koneissa ei käyttöjärjestelmiä vaihdettu, joten muutama Windows XP jäi yritykseen pyörimään. Windows 7 -järjestelmä soveltuu parhaiten yrityskäyttöön. Siitä löytyvät valmiiksi työkalut suureen osaan varmuuskopioinnista, sekä Microsoftin oma etäkäyttö-ohjelma.

Tarvittiin myös Office-tyyppinen ohjelma. Vaihtoehtoja oli kaksi: Microsoftin oma Microsoft-office sekä ilmainen Oraclen OpenOffice. Tässä päädyimme valitsemaan Microsoftin tuotteen sen paremman käyttöliittymän ja laajemman tiedostotyyppivalikoiman vuoksi. Microsoft Officen tietoturva on myös huomattavasti laajempi. Siinä on mm. ”protected view” -moodi, joka estää epämääräisten sähköpostiliitetiedostojen käynnistämästä makroja tai muita mahdollisesti haitallisia koodinpätkiä. Lisäksi henkilökunta oli tottunut käyttämään Microsoft Officea, joten uuden ohjelman opettelu olisi ollut turhaa ajanhukkaa.

Laskutus- ja potilastietokantajärjestelmänä käytettiin Receptumin Helmi-ohjelmistoa. Ohjelma kattaa kaiken, mitä potilaan hoitoon ja laskutukseen tarvitaan. Receptum toimitti tämän ohjelmiston asennuksen ja huollon.

Röntgen- ja 3D-kuvaus ohjelmana käytettiin Planmecan toimittamaa Romexis-ohjelmistoa. Ennen käytössä ollut kuvausohjelma poistuu, mutta koska vanhoja kuvia pitää silti vielä pystyä katsomaan, niin vanhan ohjelman kuvankatseluohjema säilytettiin pakon edessä.

Romexis-ohjelmisto kattaa 2D- ja 3D-kuvien muodostamisen katselun ja käsittelyn. Ohjelma tukee useita tiedostotyyppejä. Ohjelmasta löytyy myös iPhone- ja iPad-sovellukset, jolloin kuvia voi oikeastaan katsella mistäpäin maailmaa tahansa. Tämän lisäksi ohjelmistolla voi säätää tuolien instrumenttiasetuksia ja hoitoasentoa (9). Ainoana huonona puolena ohjelmassa näkisin, että se on toteutettu Javalla. Romexis-asiakasohjelmistot asennettiin jokaisen hammaslääkärin tietokoneeseen ja serveriohjelmisto asennettiin vanhaan palvelinkoneeseen.

Uudet hammaslääkärituolit olivat myös hankittu Planmeca Oy:ltä. Näissä tuoleissa on sisäänrakennettuna tietokone, joka pyörii Windows XP -käyttöjärjestelmällä. Kyseisillä koneilla ohjataan tuolin toimintaa, sekä katsellaan mm. röntgenkuvia. Koneet piti kytkeä verkkoon, mutta niissä ei alun perin ollut minkäänlaista tietoturvaa. Asensimme niihin väliaikaisesti Microsoft security essentialssin, ja kytkin Windowsin palomuurin käyttöön, jotta uskalsin altistaa ne verkon vaaroille. Seuraavalla sivulla on kuva hammaslääkärin tuolista eli koko yritystoimin sydämestä.

Kuva 9 Planmeca Sovereign -hammaslääkärituoli

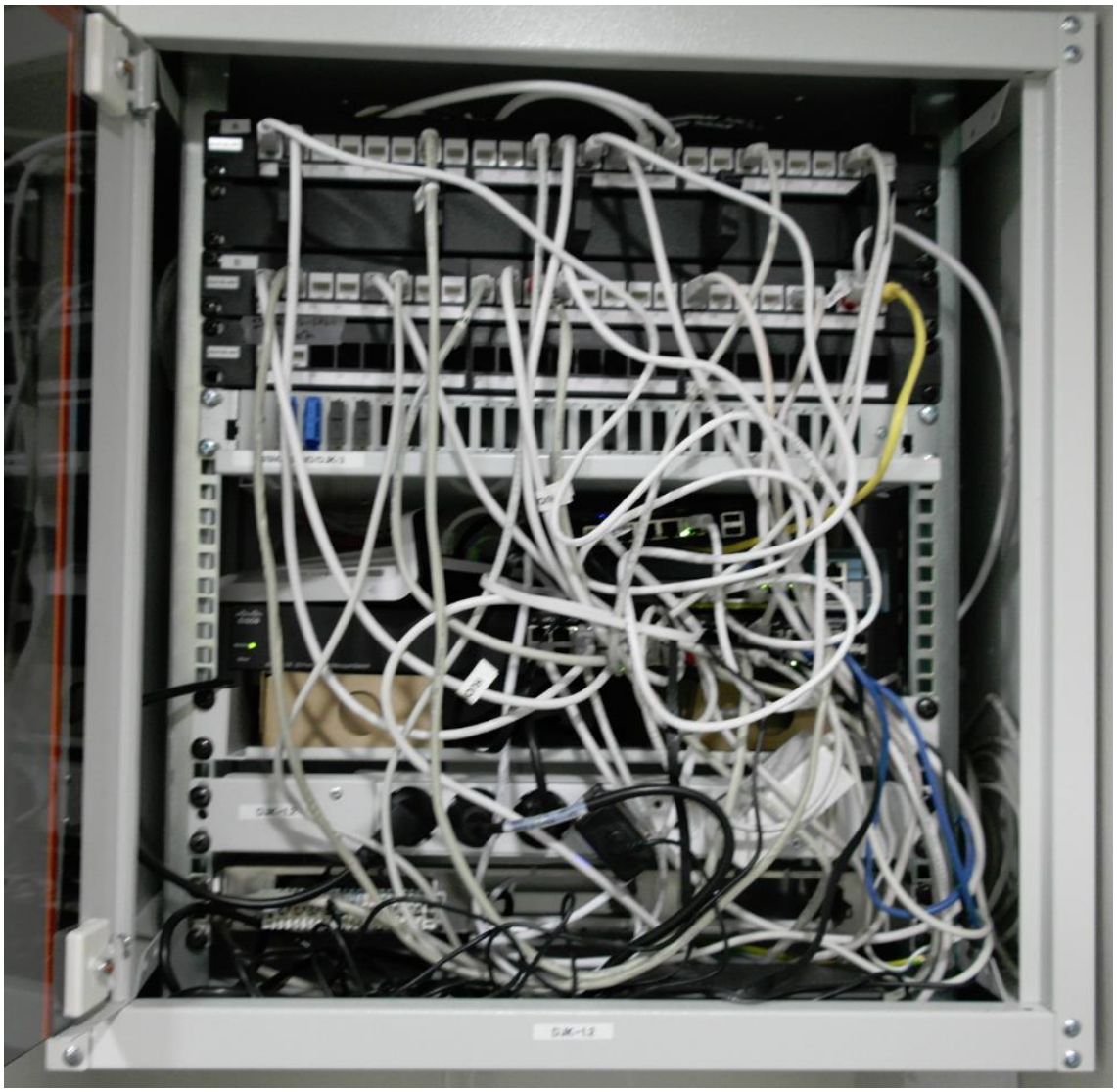
5 Yhteenveto

Työ suoritettiin vuoden 2012 kesästä vuoden 2013 tammikuuhun, jolloin viimeiset ongelmat oli hiottu pois.

Projekti alkoi suunnitelmilla, joita jalostettiin muutaman kuukauden ajan. Lopputulos oli yllättävän lähellä alkuperäisiä suunnitelmia. Suunnittelun jälkeen oli tarjouspyyntöjen aika. Tarvitsimme koneita ja ohjelmia.

Koneiden osalta lähetimme tarjouspyyntöjä paikallisille ja suuremmille tekijöille. Aikaa vastaukseen varasimme kaksi viikkoa. Määräajan sulkeutuessa kaikkiin tarjouspyyntöihin oli vastattu, ja valitsimme yrittäjän kanssa parhaan tarjouksen. Ohjelmistojen osalta tarjouspyyntikilpamme oli huomattavasti pienempi. Ohjelmat olimme suunnitteluvaiheessa jo valinneet, joten ostimme ohjelmat niiden tekijöiltä.

Laitteiden saapuessa paikalle alkoi asennus. Tämä tapahtui samaan aikaan putki- ja sähköasennusten kanssa, joten tungosta riitti eikä välillä saanut sähköä mistään. Laitteiden asentaminen oli nopea vaihe. Viimeinen tulostin oli paikallaan kaksi päivää asennuksen alkamisesta. Uusissa tiloissa oli vihdoin kunnon kytkinlaatikko, joten verkkoinfran laittaminen oli siistiä ja nopeaa. Kuvassa 10 on puolivalmiskytkinlaatikko.



Kuva 10 Puolivalmis kytkinlaatikko

Ohjelmistojen asentaminen veikin sitten aikaa. Käytännössä joka kone jouduttiin käymään läpi. Uusissa koneissa kaikki piti asentaa ja vanhoissa koneissa ohjelmia piti lisätä ja poistaa. Tämän lisäksi esimerkiksi verkkoasetukset piti laittaa joka koneeseen.

Kun kaikki oli asennettuna, alkoi ongelmien selvittely. Olin unohtanut hankkia Cisco ASA 5505:seen 50 käyttäjän lisenssin, joten tietokoneiden putoilu verkosta aiheutti päänvaivaa alussa. Suurimmaksi ongelmaksi muodostui vanha röntgen- ja 3D-kuvausohjelmisto. Vaikka ohjelmaa olikin vaihdettu, niin silti vanhoja kuvia piti pystyä katsomaan. Tämän johdosta sovimme vanhan ohjelman toimittajan kanssa, että saisimme käyttää

”trial” -avainta vanhojen kuvien katseluun. Ratkaisu oli muuten toimiva, mutta avain kestää vain 3 kk, joten neljä kertaa vuodessa joudumme pyytämään sähköpostilla uusia avaimia koneisiin, joissa pitää vanhoja kuvia nähdä.

Keväällä 2013 yrityksen tietoverkko ja laitteisto toimivat moitteetta. Järjestelmän suunnittelu ja toteutus onnistuivat niin hyvin, että ylläpitoon vaadittavat IT-resurssit ovat minimaaliset. Käytännössä Mediuksessa käy yksi IT-henkilö kerran kuussa.

Lähteet

1 Reititin. Verkkodokumentti. Wikipedia.
<http://fi.wikipedia.org/wiki/Reititin> (luettu 10.3.2014)

2 Kykin. Verkkodokumentti. Wikipedia.
<http://fi.wikipedia.org/wiki/Kytkin_%28tietoliikenne%29> (luettu 10.3.2014)

3 VPN. Verkkodokumentti. Wikipedia.
<http://fi.wikipedia.org/wiki/VPN> (luettu 16.4.2012)

4 VPN-verkot. Verkkodokumentti. 2K mediat.
<http://www.2kmediat.com/vpn/yhteys.asp> (luettu 16.4.2013)

5 IPsec. Verkkodokumentti. Wikipedia.
<http://fi.wikipedia.org/wiki/IPsec> (luettu 16.4.2013)

6 VPN software clients nad Software based VPN. Verkkodokumentti. vPNlabs.
<http://www.vpnlabs.com/vpn-software.html> (luettu 16.4.2013)

7 RAID tietotekniikka. Verkkodokumentti. Wikipedia.
<http://fi.wikipedia.org/wiki/RAID_%28tietotekniikka%29>(16.4.2013)

8 Yleisin salasana verkossa. Verkkodokumentti. MPC.
<http://www.mikropc.net/kaikki_uutiset/yleisin+salasana+verkkopalvelussa+on-masentavan+helppo/a366584> (16.4.2013)

9 Romexis. Verkkodokumentti. Planmeca.
<http://www1.planmeca.com/fi/ohjelmistot/planmeca_romexis>